UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/092,544	03/08/2002	Kenjiro Ueda	24929	8830

20529 7590 03/09/2006

NATH & ASSOCIATES
112 South West Street
Alexandria, VA 22314

EXAMINER	
BAUM, RONALD	
ART UNIT	**PAPER NUMBER**
2136	

DATE MAILED: 03/09/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/092,544	UEDA ET AL.	
	Examiner	Art Unit	
	Ronald Baum	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☐ Responsive to communication(s) filed on _____.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-3,5-8,10-13 and 17* is/are rejected.

7)☐ Claim(s) *4,9,14-16* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☒ All b)☐ Some * c)☐ None of:

1.☒ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date *02132006*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-17 are pending for examination.

2. Claims 1-3,5-8,10-13,17 are rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

3. Claims 1-3,5-8,10-13,17 are rejected under 35 U.S.C. 102(e) as being anticipated by Dömstedt, U.S. Patent 6,845,159 B1.

4. As per claim 1; "An encryption method for encrypting information including

a plurality of continuous unit blocks having a reproduction order,

said plurality of unit blocks being encrypted

one unit block at a time [figures 1-7 and accompanying descriptions, and more particularly col. 2,lines 18-col. 3,line 34, whereas the actual pre and post 'converting' block/stream/stored memory processing (i.e., table setup and storage and transfer thereof), clearly encompasses the claim limitations, as broadly interpreted by the examiner.],

wherein a seed of an encryption key for encrypting a unit block is based

on one or more unit blocks that are, in the reproduction order,

before the unit block or

on information generated by encrypting one or more unit blocks

before the unit block [figures 1-7 and accompanying descriptions, and more particularly col. 2,lines 18-col. 3,line 34, col. 8,lines 35-col. 9,line 33, whereas the use of data that is a function of the input information (i.e., information pieces, block/stream/stored memory content, etc.,) to form the basis of the cryptographic functions/services (i.e., references of operations/instructions in the table lookup used for encryption/decryption key generation information via a single unit/block, or iteratively processed in a chaining scenario), clearly encompasses the claim limitations, as broadly interpreted by the examiner.].".

As per claim 6, this claim is the decryption side of the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection, given the cryptographic functions/services (i.e., references of operations/instructions in the table lookup used for encryption/decryption key generation information) encompasses the decryption as well as the encryption aspects; "A decryption method for decrypting information including

a plurality of continuous encrypted unit blocks having a reproduction order,

said plurality of encrypted unit blocks having being encrypted

one unit block at a time,

wherein a seed of an encryption key for decrypting an encrypted unit block is based

on one or more unit blocks that are, in the reproduction order,

before the unit block or

on information generated by encrypting one or more unit blocks

before the unit block.".

As per claim 11, this claim is the apparatus claim for the method claims 1,6 above, and is rejected for the same reasons provided for the claim 1,6 rejection; "A recording and reproducing apparatus comprising:

encrypting means for encrypting information including

a plurality of continuous unit blocks having a reproduction order,

one unit block at a time;

recording means for recording the encrypted information

on a recording medium; and

decrypting means for decrypting

the plurality of encrypted unit blocks for reproduction,

one unit block at a time,

which are the encrypted information read from said recording medium, wherein

a seed of an encryption key for encrypting a unit block and

a seed of an encryption key for decrypting an encrypted unit block are based

on one or more unit blocks that are, in the reproduction order,

before the unit block or

on information generated by encrypting one or more unit blocks

before the unit block.".

5. Claim 2 ***additionally recites*** the limitation that; "The encryption method according to claim 1,

wherein the seed of the encryption key is chained at least twice.".

The teachings of Dömstedt are directed towards such limitations (i.e., figures 1-7 and accompanying descriptions, and more particularly col. 2,lines 18-col. 3,line 34, col. 8,lines 35-col. 9,line 33, whereas the cryptographic functions/services (i.e., initial input sequence for a key, seed, etc., for encryption/decryption generation information via a single unit/block, or iteratively (i.e., at least twice) processed 'generating a large number of different keys from a single seed. ... achieved simply by repeating the program defined by the seed' in a chaining 'before the unit block' scenario), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

As per claim 7, this claim is the decryption side of the method claim 2 above, and is rejected for the same reasons provided for the claim 2 rejection, given the cryptographic functions/services (i.e., references of operations/instructions in the table lookup used for encryption/decryption key generation information) encompasses the decryption as well as the encryption aspects; "The decryption method according to claim 6,

wherein the seed of the encryption key is

chained at least twice.".

As per claim 12, this claim is the apparatus claim for the method claims 2,7 above, and is rejected for the same reasons provided for the claim 2,7 rejection; "The recording and reproducing apparatus according to claim 11,

wherein the seed of the encryption key is

chained at least twice.".

6. Claim 3 ***additionally recites*** the limitation that; "The encryption method according to claim 2,

wherein the chain is reset when the seed is

chained a predetermined number of times.".

The teachings of Dömstedt are directed towards such limitations (i.e., figures 1-7 and accompanying descriptions, and more particularly col. 2,lines 18-col. 3,line 34, col. 8,lines 35-col. 9,line 33, whereas the cryptographic functions/services (i.e., key, seed, etc., generation/processing via iterative unit/block processing in a chaining scenario is inherently self limiting), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

As per claim 8, this claim is the decryption side of the method claim 3 above, and is rejected for the same reasons provided for the claim 3 rejection, given the cryptographic functions/services (i.e., references of operations/instructions in the table lookup used for encryption/decryption key generation information) encompasses the decryption as well as the encryption aspects; "The decryption method according to claim 7,

wherein the chain is reset when the seed is

chained a predetermined number of times.".

As per claim 13, this claim is the apparatus claim for the method claims 3,8 above, and is rejected for the same reasons provided for the claim 3,8 rejection; "The recording and reproducing apparatus according to claim 12,

wherein the chain is reset when the seed is

chained a predetermined number of times.".

7. As per claim 5; "An encryption method for encrypting information including

a plurality of continuous unit blocks having a reproduction order,

said plurality of unit blocks being encrypted

one unit block at a time [figures 1-7 and accompanying descriptions, and more particularly col. 2,lines 18-col. 3,line 34, whereas the actual pre and post 'converting' block/stream/stored memory processing (i.e., table setup and storage and transfer thereof), clearly encompasses the claim limitations, as broadly interpreted by the examiner.],

wherein a seed of an encryption key for encrypting a unit block is

information based on an encryption key used for

encrypting a unit block that is, in the reproduction order,

before the unit block to be encrypted [figures 1-7 and accompanying descriptions, and more particularly col. 2,lines 18-col. 3,line 34, col. 8,lines 35-col. 9,line 33, whereas the use of data that is a

function of the input information (i.e., information pieces, block/stream/stored memory content, etc.,) to form the basis of the cryptographic functions/services (i.e., references of operations/instructions in the table lookup used for encryption/decryption key (i.e., initial input sequence for a key, seed, etc.,) generation information via a single unit/block, or iteratively processed in a chaining 'before the unit block' scenario), clearly encompasses the claim limitations, as broadly interpreted by the examiner.].".

As per claim 10, this claim is the decryption side of the method claim 5 above, and is rejected for the same reasons provided for the claim 5 rejection, given the cryptographic functions/services (i.e., references of operations/instructions in the table lookup used for encryption/decryption key generation information) encompasses the decryption as well as the encryption aspects; "A decryption method for decrypting information including

a plurality of continuous encrypted unit blocks having a reproduction order,

said plurality of encrypted unit blocks having being encrypted

one unit block at a time,

wherein a seed of an encryption key for decrypting an encrypted unit block is information based

on an encryption key used for decrypting a unit block that is, in the reproduction order,

before the unit block to be decrypted.".

As per claim 17, this claim is the apparatus claim for the method claims 5,10 above, and is rejected for the same reasons provided for the claim 5,10 rejection; "A recording and reproducing apparatus comprising:

encrypting means for encrypting information including

a plurality of continuous unit blocks having a reproduction order,

one unit block at a time;

recording means for recording the encrypted information

on a recording medium; and

decrypting means for decrypting

the plurality of encrypted unit blocks for reproduction,

one unit block at a time,

which are the encrypted information read from said recording medium, wherein

a seed of an encryption key for encrypting a unit block and

a seed of an encryption key for decrypting an encrypted unit block

are information based on an encryption key used for

encrypting a unit block that is, in the reproduction order,

before the unit block to be encrypted or decrypted.".

Allowable Subject Matter

Claims 4,9,14-16 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

8. Claim 4 ***additionally recites*** the limitation that; "The encryption method according to claim 2,

wherein an initial value IV of a seed of an encryption key used for

encrypting a first unit block of the plurality of unit blocks

having the reproduction order is stored,

wherein the chain has a plurality of hierarchy levels,

a first hierarchy level is encrypted based on

the initial value IV of the seed of the encryption key, and

a second and higher hierarchy levels are encrypted based on

a seed of an encryption key at a lower hierarchy level,

wherein, when encrypted unit blocks from

the first unit block to

any given unit block of the encrypted information are decrypted for reproduction,

the initial value IV of the seed of

the encryption key that was stored is used, and

wherein, when the reproduction of the unit blocks to the given unit block ends,

the initial value IV of the seed of

the encryption key that was stored is

erased and

both

a seed of an encryption key used for encrypting a unit block

follows the given unit block in the reproduction order and

a seed of an encryption key used for encrypting a unit block

at another hierarchy level after the given unit block

are stored.".

As per claim 9, this claim is the decryption side of the method claim 4 above, given the cryptographic functions/services (i.e., references of operations/instructions in the table lookup used for encryption/decryption key generation information) encompasses the decryption as well as the encryption aspects; "The decryption method according to claim 7,

wherein an initial value IV of a seed of an encryption key used for

encrypting a first unit block of the plurality of unit blocks

having the reproduction order is stored,

wherein the chain has a plurality of hierarchy levels,

a first hierarchy level is encrypted based on

the initial value IV of the seed of the encryption key, and

a second and higher hierarchy levels are encrypted based on

a seed of an encryption key at a lower hierarchy level,

wherein, when encrypted unit blocks from

the first unit block to

any given unit block of the encrypted information are decrypted for reproduction,

the initial value IV of the seed of

the encryption key that was stored is used, and

wherein, when the reproduction of the unit blocks to the given unit block ends,

the initial value IV of the seed of

the encryption key that was stored is

erased and

both

a seed of an encryption key used for encrypting a unit block that

follows the given unit block in the reproduction order and

a seed of an encryption key used for encrypting a unit block

at another hierarchy level after the given unit block

are stored.".

As per claim 16, this claim is the apparatus claim for the method claims 4,9 above; "The recording and reproducing apparatus according to claim 12, further comprising:

storage means for storing

an initial value IV of a seed of an encryption key used for

encrypting a first unit block of the plurality of unit blocks

having the reproduction order,

wherein the chain has a plurality of hierarchy levels,

a first hierarchy level is encrypted based on

the initial value IV of the seed of the encryption key, and

a second and higher hierarchy levels are encrypted based on

a seed of an encryption key at a lower hierarchy level,

wherein, when encrypted unit blocks from

the first unit block to

any given unit block of the encrypted information are decrypted for reproduction,

the initial value IV of the seed of

the encryption key that stored in said storage means is used, and

wherein, when the reproduction of the unit blocks to the given unit block ends,

the initial value IV of the seed of

the encryption key is

erased from said storage means and

both

a seed of an encryption key used for encrypting a unit block that

follows the given unit block in the reproduction order and

a seed of an encryption key used for encrypting a unit block

at another hierarchy level after the given unit block are stored in said storage means.".

9. Claim 14 ***additionally recites*** the limitation that; "The recording and reproducing apparatus according to claim 11, further comprising:

storage means for storing an initial value IV of a seed of an encryption key used for

encrypting a first unit block of the plurality of unit blocks

having the reproduction order,

wherein the initial value IV of the seed of the encryption key stored in said storage means is used when

the first unit block of the plurality of unit blocks

encrypted by said encrypting means and

having the reproduction order

is decrypted for reproduction.".

10. Claim 15 ***additionally recites*** the limitation that; "The recording and reproducing apparatus according to claim 11, further comprising:

storage means for storing an initial value IV of a seed of an encryption key used for

encrypting a first unit block of the plurality of unit blocks

having the reproduction order,

wherein, when encrypted unit blocks from

the first unit block to

any given unit block, which are the encrypted information, are decrypted for reproduction,

the initial value IV of the seed of

the encryption key that was stored in said storage means is

used, and

wherein, when the reproduction of the unit blocks to the given unit block ends,

the initial value IV of

the seed of the encryption key is

erased from said storage means and

a seed of an encryption key used for encrypting

a unit block that follows the given unit block in the

reproduction order is

stored.".

Conclusion

11. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner

3/6/06

CHRISTOPHER REVAK
PRIMARY EXAMINER